International Journal of Information Security
https://doi.org/10.1007/s10207-023-00810-y

REGULAR CONTRIBUTION

Maritime decision-makers and cyber security: deck officers' perception of cyber risks towards IT and OT systems

Marie Haugli-Sandvik[1] · **Mass Soldal Lund**[2] · **Frøy Birte Bjørneseth**[1,3]

Accepted: 24 December 2023

Abstract
Through a quantitative study of deck officers' cyber risk perceptions towards information (IT) and operational (OT) systems, this paper contributes to substantiate the importance of considering human behaviour within maritime cyber security. Using survey data from 293 deck officers working on offshore vessels, statistical analyses were conducted to measure and predict the participants cyber risk perceptions towards IT and OT systems. Performing a Wilcoxon signed-rank test revealed a significant discrepancy in the levels of cyber risk perception between the system categories. Hierarchical regression analyses were conducted to develop statistical models, considering multiple independent variables, including perceived benefit, cyber security training, experience with cyber-attacks, and trust towards various stakeholders. Key findings revealed distinct results for IT and OT systems, and the regression models varied in both predictive power and significance of the independent variables. Perceived benefit positively predicts deck officers cyber risk perception for both IT and OT systems, while trust, which included measures of social trust and confidence, was not found to be significant. Cyber security training and experience with cyber-attacks only influence deck officers' perception of cyber risks related to operational technology. Practical implications of this work provide actionable recommendations for the maritime industry, including tailored risk communication tools, training programs, reporting systems, and holistic policies.

Keywords Maritime cyber security · Cyber risk perception · IT and OT systems · Perceived benefit · Trust · Cyber security training

1 Introduction

In the aftermath of rapid digitalisation, which was further accelerated by the global COVID-19 pandemic, and with the war in Europe changing the cyber threat landscape, cyber-attacks have emerged as a mounting concern for the offshore industry [1]. The maritime sector, with its extensive reliance on interconnected systems, is particularly vulnerable to such threats [2]. A well-known example of a cyber-attack in the maritime industry was the ransomware NotPetya hitting the Maersk Shipping Company in 2017, resulting in a company loss of over 300 million USD [3]. Another notable cyber-attack occurred at the International Maritime Organization (IMO) in 2020, disrupting their systems shortly before the launch of their resolution on enhancing maritime cyber risk management [4]. Recent reports and papers provide an overview of cyber-attacks against both shipping companies and vessels, leaving no doubt that maritime cyber risks are omnipresent [5–7].

Consequently, there is a growing concern about the vulnerabilities inherent in maritime information and operational technology systems (IT and OT systems), and potential consequences of successful cyber-attacks targeting these systems range from substantial financial losses to environmental disasters and the potential loss of life at sea [8]. Safeguarding the integrity, confidentiality, and availability of critical maritime systems has become an essential task for industry stakeholders [9], especially in regard to the operational technology which governs offshore vessels physical assets [3].

✉ Marie Haugli-Sandvik
marie.h.sandvik@ntnu.no

1 Department of Ocean Operations and Civil Engineering, Norwegian University of Science and Technology, 6025 Aalesund, Norway

2 Inland Norway University of Applied Sciences, 2450 Rena, Norway

3 Kongsberg Maritime, 6025 Aalesund, Norway

Published online: 02 February 2024

At sea, the human operator plays a crucial role in the first line defence against cyber risks [10]. Previous research highlights the importance of comprehending human behaviour to develop precise tools for cyber risk mitigation strategies within the maritime domain [11–13]. In this regard, one important aspect within behaviour science is the concept of risk perception, which investigates how various factors influence the perception of technological risk across different contexts [14]. It is widely recognized that action-related decisions build on individual risk perceptions, and that these perceptions play a major role in prompting protective action towards cyber risks [15, 16]. Consequently, with the new cyber threat landscape that modern vessels must navigate today, it is of utter importance to help the crew prevent and handle cyber incidents. To do this effectively, it is vital to investigate maritime decision-makers', such as deck officers, cyber risk perceptions towards IT and OT systems [17, 18]. The nature of IT and OT is different, and cyber risk management strategies must consider this distinction, especially to strengthen maritime OT-security and facilitate good cyber security behaviour [3, 9].

Motivated by a previous qualitative study that explored factors influencing deck officers' perception of cyber risks [19], this paper aims to investigate variations and causal relationships in cyber risk perception within this maritime context. The objective of this study is twofold: to measure deck officers' cyber risk perception and develop predictive statistical models to predict their perception of cyber risks towards IT and OT systems. To achieve this, a survey was conducted among deck officers working on offshore vessels within Norwegian shipping companies. The survey included measures of cyber risk perception, perceived benefit, cyber security training, experience with cyber-attacks, and trust towards different stakeholders within the maritime domain. The results have potential to further inform decision-making processes and facilitate development of targeted and preventive measures to enhance maritime cyber security and safety.

The remaining sections of this paper are organized as follows: first, theoretical aspects and previous research is presented, followed by the hypotheses investigated in this paper. Subsequently, the methodology is presented before the results are given and discussed. Finally, the limitations are addressed before concluding the paper, which also includes suggestions for further research.

2 Theoretical aspects

2.1 Maritime cyber security and cyber risks

The unique characteristics of the maritime domain, such as global operations, long supply chains, operational and demanding working environments, and diverse stakeholders, pose significant challenges in building and maintaining robust cyber security [5]. The offshore industry is experiencing rapid changes, driven by simultaneous efforts to achieve the green shift while aiming to reduce operational costs. This has led to a growing emphasis on digitalization and automation as essential marked strategies to maintain relevance [20]. Vessels, equipped with advanced technologies and automated systems, are connected through the Internet of Things (IoT), satellite communications, and cloud-based services. The IT-infrastructure is becoming more advanced, and the previous air gap isolating operational technology is closing as propulsion, machinery and navigational systems becomes more networked and connected [3]. This complexity and interconnectedness increases the cyber-attack surface, leaving vessels and crew exposed to cyber risks caused by threats exploiting cyberspace [21].

Maritime cyber security can be understood as the measures and practices implemented to protect vessels, ports, shipping companies and related infrastructures from cyber risks [9]. By use of von Solms' and van Niekerk's [22] definition of cyber security, this understanding involves the protection of cyberspace itself, the electronic information, the IT and OT systems that support cyberspace, and the users of cyberspace. The users, in this context the crew, are vital assets that needs protection and safeguarding at sea. As emphasized in earlier research, safety and security are intertwined with each other, making maritime cyber risks potential safety risks and vice versa [11].

Research within maritime cyber security has increased over the last decade, and several recent studies focus on aspects related to cyber security awareness [6]. These studies often focus on cyber preparedness in maritime companies [23], seafarers' level of cyber security awareness [24], or how training frameworks can be developed to enhance awareness and knowledge [12, 25]. While such studies are centred around the human aspect of cyber security, they often fell short of addressing the underlying behavioural processes such as risk perception.

Despite the growing interest and awareness of cyber risks and threats in the maritime sector, findings of Chubb et al. [26] suggest that seafarers and other industry professionals are still struggling with comprehending cyber risks and the implementation of mitigating measures. Some may underestimate the potential impact of cyber incidents due to a lack of training and experience with cyber-attacks, while others may be overwhelmed by the complexities of cyber threats and uncertain about the appropriate risk mitigation strategies [5, 24]. Understanding cyber risk perception and factors influencing them, can help foster a proactive and resilient cyber risk management approach within maritime companies. This study includes measures of cyber security training

and experience with cyber-attacks to investigate their causal relationship to deck officers' perception of cyber risks.

2.2 IT and OT systems

Offshore vessels rely extensively on a diverse range of information technology (IT) and operational technology (OT) systems to support their operational activities [3]. IT systems encompass the traditional computing and networking infrastructure used for administrative tasks, communication, data management, and business operations within shipping companies, their vessels, and ports. These systems often handle sensitive information such as financial data, crew details, and cargo manifests. On the other hand, OT systems refer to the hardware and software that control, monitor, and automate the physical processes and machinery in maritime operations, such as navigational systems, engine controls, cargo handling equipment, and safety mechanisms [27].

The key difference between IT and OT systems lies in their primary functions and scope of influence. While IT systems are predominantly focused on data management and administrative functions, OT systems are specifically designed to interact with and control physical assets and processes [9]. These systems are vital for ensuring the safe and efficient operation of vessels. However, as mentioned above, the integration and digitalization of these systems introduce new cyber risks.

Reviewed literature shows the omnipresence of cyber risks towards modern vessels [5]. Several recent papers provide records of inherent system vulnerabilities, possible cyber-attack vectors and significant previous cyber-attacks against vessels and maritime industry [1, 2, 4, 6, 7, 27]. It is a clear trend that connectivity and interconnection affect the security level of maritime infrastructures negatively. Moreover, a lack of proper cyber security training and more sophisticated cyber-attack methods increases the probability of successful cyber-attacks towards vessels and maritime industry [6]. Additionally, studies show that there is a lack of OT-security expertise within shipping companies, and that it remains ambiguity about the allocation of responsibility for securing the operational technology [26].

Research within maritime cyber security has increased over the years. Recently, there has been a shift in focus from mainly looking at cyber risks towards information technologies, to a greater interest in cyber risks and threats towards operational technologies as well [3, 26, 28]. Even so, few papers address human behaviour within maritime cyber security, regardless of the well-established fact that humans play an important role in cyber security and protection of all technical systems [8, 11]. How deck officers perceive cyber risks towards IT and OT systems will influence their behaviour and cyber security compliance [19]. Since the two system categories have fundamentally distinct functions and history

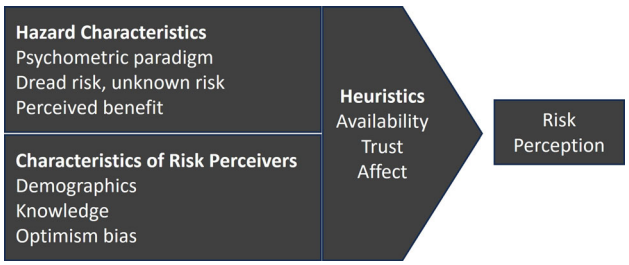

Fig. 1 Paradigms and influential factors in risk perception (adapted from Siegrist and Árvai, 2020) [32]

of digitalization, different factors might influence the officer's perception of risks towards these systems. Therefore, the objective in this study is to measure their level of cyber risk perception towards IT and OT systems, and to test the causal relationship between their perceptions and independent variables as perceived benefit and trust.

2.3 Risk perception

Since the 1970s, researchers have been studying how risk perceptions are formed, trying to explain how people reconstruct previously assimilated risk through subjective judgements [29–31]. How people perceive risk is important because it influences individual behaviour as well as the acceptance and commitment to technology, policies, and norms [32]. Each technology has its specific risk factors that need to be studied in their own right and context [33], especially since factors explaining people's perception of risk varies from population to population and from profession to profession [34, 35].

As shown in Fig. 1, there are multiple paradigms within risk perception research, and Siegrist and Árvai (2020) group these within three general approaches: hazard characteristics, characteristics of risk perceivers, and heuristics. Within these approaches, studies of risk perception related to perceived benefit, trust, and the availability heuristic can be found. These factors have been identified as predictive factors of cyber risk perceptions in various research fields [11, 19].

2.3.1 Perceived benefit of technology

The studies of Starr (1969) and Fischoff et al. (1979) have been the inspiration for numerous of perceived risk and benefit studies within the psychological paradigm of risk perception [36]. Starr advocated for a "revealed preference" approach where use of risk and benefit data could be used to reveal patterns of acceptable risk–benefit trade-offs [37]. Some years later, in the wake of the debate over Starr's approach, Fischoff et al. [31] developed the "expressed preference" approach which indicates that society may accept higher levels of risk with more beneficial activities and tolerate higher risk levels for voluntary activities [38]. This

coincides with several studies finding an inverse correlation between levels of cyber risks towards information technologies and internet-related activities perceived as beneficial [15, 38–40].

The causal relationship between perceived risk and benefit have been questioned and it is postulated that risk and benefit perceptions may be influenced by other variables or causal relationships, as within the psychometric paradigm [29, 41]. This study will investigate to what extent perceived system benefit has a causal relationship with deck officers cyber risk perception.

2.3.2 Trust

An often used definition of trust within risk perception and management: *"Trust is a psychological state compromising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another"* [42]. According to Siegrist [35], trust is an important concept for a better understanding of perceptions or decisions made in the risk domain, and the function of trust can be a mechanism for reduced complexity that enables people to maintain their capacity to act in a complex environment. This coincides with a study indicating that the concept of trust could be of relevance to deck officers' perception of cyber risks and their vessels' cyber defence [19].

One way of classifying trust mechanisms is by looking at trust as the result of social trust and confidence. This conceptual framework of trust postulates that social trust is related to the judgement of similarities in intentions and values, whereas confidence is based on past experiences suggesting that future events will occur as expected [43]. Previous studies using this framework often ask participants to assess their trust in an industry or such, but it can be unclear to what extent the participants rely on competence or value aspects when answering such questions [44]. Because social trust and confidence often is found to be strongly correlated [35], they will be combined into one construct in this study [45].

The importance of trust is somewhat controversial, and previous research have found various degrees of correlation between trust measurements and risk perceptions of technology [46]. It seems that degree of knowledge about the technology and risks involved, the perceived importance of the issue, and the methods used to measure the constructs of trust is important for the observed correlation between trust and risk perception [35]. Other research findings question if the effect of trust is direct or indirect, and that trust influences both risk and benefit perceptions. Social trust has been found to decrease risk perceptions and increase benefits association [41, 47].

2.3.3 The availability heuristic

People often rely on heuristics when making decisions, meaning they replace a target attribute that is not readily accessible (e.g., the objective probability of a cyber-attack) with a heuristic that comes to mind more easily (e.g., the number of concrete examples of cyber-attacks that can be recalled) [32, 48]. In the risk domain, a major part of research focus on the availability heuristic [35], which is when people use the "ease with which instances of occurrences can be brought to mind" [49].

If people rely on the availability heuristic, they tend to perceive threats or risk events as high risk when they find it easy to imagine, recall or conceptualise the occurrence of such threats or events [50, 51]. How heuristics are used to evaluate information and how these processes influence certain cognitive biases, has played an important role in the discussion of risk perception [30]. Nevertheless, how the availability heuristic should be operationalized or measured is undetermined, and it may not be fully clear in which situations and contexts people actually rely on this heuristic [32].

3 Purpose of study and hypotheses

The aim of the research presented in this paper is to measure deck officers' cyber risk perceptions and develop statistical models for prediction of their perception of cyber risks towards their vessels IT and OT systems. Informed by previous research and theory within the fields of maritime cyber security and risk perception, the following two hypotheses were developed:

- H1: Deck officers perceive lower cyber risks towards OT systems than IT systems.
- H2: There is a difference in how the independent variables perceived benefit, trust, cyber security training, and experience with cyber-attacks predict deck officers' cyber risk perception towards their vessels IT and OT systems.

This study was motivated by a previous qualitative study conducted to explore and describe factors influencing deck officers' perception of cyber risks [19]. Several main themes that emerged from those in-depth interviews, directly inspired the hypotheses development in this study. For instance, the qualitative findings implied that deck officers rely on trust in other stakeholders for cyber defence. Furthermore, the officers emphasized having limited cyber security knowledge and training, and they described IT and OT systems differently with regard to cyber risks and perceived benefits [19]. By grounding the hypotheses in the real-world experiences of deck officers, layers of context and

depth were added to the research design, ensuring relevance to practical challenges faced by maritime decision makers.

4 Method

To investigate the hypotheses, a survey was conducted among deck officers working on offshore vessels within Norwegian shipping companies. The survey included measures of cyber risk perception, perceived benefit, and trust towards different stakeholders in relation to their vessels IT and OT systems. Participants were also asked about their experience with cyber-attacks and amount of cyber security training. The constructs in the questionnaire were developed based on previous research within maritime cyber security and cyber risk perception [11, 19]. Wilcoxon signed-rank test was used to compare the level of perceived cyber risk towards IT and OT systems. Then, hierarchical regression analyses were performed to test the independent variables prediction of cyber risk perception.

4.1 Participants

The participants in this study were selected to gain insights into cyber risk perception in the offshore industry. The selection criteria were deck officers employed on offshore vessels, which are vessels that specifically serve operational purposes such as oil exploration and construction work at the high seas [52]. Offshore vessels operate in a critical environment and utilize highly technical systems, making cyber risk management of utmost importance [3]. To ensure adequate representation, an online survey was distributed to eleven of the largest offshore companies operating in Norway. These companies were responsible for distributing the survey among their deck officers working on offshore vessels during the designated period between October and December 2022.

To ensure sample representativeness, efforts were made to recruit participants who were representative of the target population of deck officers working on offshore vessels. Although the study did not employ random sampling, the sample characteristics closely mirrored those of the broader population in terms of demographic and professional attributes. This enhances the external validity and generalizability of the findings to the wider population [53].

Prior to participating in the study, the participants were provided with information regarding the purpose of the research. They were explicitly informed that the survey was anonymous, ensuring that their responses could not be traced back to them. Participants were requested to confirm their voluntary consent to participate, thereby acknowledging their understanding of the study's objectives. To address potential concerns or seek additional information or support, participants were also provided with contact information of the researchers. These measures were implemented to uphold ethical standards and to safeguard participant confidentiality and privacy throughout the research process.

4.2 Questionnaire

The questionnaire used in this study consisted of five sections: (1) demographic information, (2) perception of system benefits, (3) experience with cyber-attacks and cyber security training, (4) perception of cyber risks, and (5) trust towards different stakeholders. See appendix for an overview of the questionnaire wording, which was distributed in both English and Norwegian to the participants.

The first section included questions about age range, gender, educational level, years of experience working at sea, and what rank they currently were holding on their offshore vessel. Section two included questions about assessing the benefits of systems deck officers depend on in their everyday working life. Participants were asked to rate the level of benefit on a scale ranging from 1 (no benefit at all) to 5 (very high benefit) for systems commonly found on the bridge of an offshore vessel. They also got the option of choosing "Don't know/Don't use this" when assessing the systems.

The third section had the topics experience with cyber-attacks and cyber security training. The first questions were related to the participants experience with cyber-attacks towards their vessel and shipping company, together with how many times they have heard about others being victim of a cyber-attack. Then, the participants were asked to rate how often they have conducted different types of cyber security training (e.g., computer-based training, security drills and tabletops).

Section four included questions about assessing the level of cyber risks towards the same type of systems they rated in section two. Participants were asked to rate the level of cyber risk on a Likert scale ranging from 1 (no cyber risk at all) to 5 (very high cyber risk) or select the option "Don't know/Don't use this". The systems listed were the same as for perceived benefit, and they were presented in a random order as shown in the appendix.

Section five included questions about social trust and confidence, which forms the construct trust, in stakeholders related to securing the onboard systems and performing the cyber security tasks they are responsible for. Participants were asked to rate their level of trust on a scale ranging from 1 (no trust at all) to 5 (very high trust). The stakeholders they were asked about was their crew, management, IT-department, suppliers of onboard systems, their government, and the International Maritime Organisation (IMO).

A panel of academic experts and a small group of former deck officers with relevant expertise were involved in the

review process of the questionnaire. Their valuable insights and feedback helped refine the questionnaire to ensure its suitability and relevance to the study context. Prior to the main data collection, a pilot test of the questionnaire was conducted. A subset of participants, similar to the target population, were invited to complete the questionnaire and provide feedback. This pilot testing allowed for the identification of potential ambiguities or difficulties in item interpretation. Based on the feedback received, adjustments were made to improve the clarity of the questionnaire items, enhancing the face validity and content validity [53]. The pilot study was conducted with seven participants, and they were not included in the final sample.

The survey was administered online using the Nettskjema tool, specifically designed to meet privacy requirements in Norway [54]. The online format allowed for efficient data collection and facilitated wider accessibility for participants. The survey was accessible to the participants between the 19th of October and the 31st of December 2022, providing a designated time frame for response submission.

4.3 Statistical analyses

Significance level of $p < 0.05$ was used as limit, and all analyses were performed in version 28 of SPSS. There were no missing data as the electronic survey required mandatory answers to all the questions. Even so, the option "Don't know/Don't use this" was given the value 0 in the dataset and treated as a missing value for the constructs cyber risk perception and perceived benefit.

Wilcoxon signed-rank test was used to test for significant discrepancies between deck officers' perception of cyber risk towards IT and OT systems. This test was appropriate since it allows for testing of two conditions when the scores came from the same participants and since the statistical data is not normally distributed [53].

Two separate hierarchical linear regression analyses were performed to investigate the causal relationships between the independent variables and the dependent variables cyber risk perception towards IT systems and cyber risk perception towards OT systems. Reliability and validity of the measurements were investigated together with multicollinearity tests. Evaluation of increase or decrease in R^2 between the steps in regression analyses was used to determine significance between two consecutive steps in the analyses.

5 Results

5.1 Descriptive statistics

A total of 293 respondents participated in the study. Among the respondents, 96% identified as male (N = 282), while 2.5% identified as female (N = 7). An additional 1.5% of participants chose to identify as "other" or preferred not to disclose their gender (N = 4). Given the male-dominated nature of the offshore industry [55], the high percentage of male participants aligns with expectations. In terms of age distribution, 60.4% of participants fell within the age range of 30–49 years. Detailed statistical information about the sample can be found in Table 1.

Table 1 Basic statistics of the sample

Options	%	*n*
Gender		
Other/don't want to say	1.4	4
Male	96.2	282
Female	2.4	7
Age		
19–29	15.4	45
30–39	27.6	81
40–49	32.8	96
50–59	20.8	61
60–69	3.4	10
Rank		
Second mate	40.6	119
Chief mate	25.6	75
Captain	33.8	99
*Education**		
Vocational school	49.5	148
Bachelor's degree	44.0	129
Master's degree	14.7	43

*Participants could choose more than one option in this question

Table 2 gives an overview of the average level of cyber risk and benefit the deck officers perceived of each system in the questionnaire, together with statistics of how many participants answering "Don't know/Don't use this". One of the IT systems (passenger servicing and management systems) scored high on "Don't know/Don't use this" (39.2% under perceived benefit and 43.3% when assessing cyber risks), so it was excluded in the analyses.

5.2 Wilcoxon signed-rank test

Wilcoxon signed-rank test was conducted to examine significant discrepancies in the deck officers' levels of cyber risk perception towards IT and OT systems. Because one IT system was excluded from the analysis, summative indexes with mean values were used in this test (Table 3). The result is conveyed in Table 4 and revealed that deck officers perceive a significant lower cyber risk towards OT systems (Mean = 2.69) than IT systems (Mean = 3.44), $z = -11.97$, $p = 0.00$, $r = -0.703$. This confirmed H1 and the divide between these two system categories were kept when performing the regression analysis.

Table 2 Descriptive statistics of IT and OT systems

	Mean cyber risk	*N**	%*	Mean benefit	*N***	%**
IT system						
E-mail	4.38	3	1.0	4.82	1	0.3
Passenger servicing and management systems***	3.03	127	43.3	3.69	115	39.2
Remote access for monitoring	3.48	39	13.3	3.62	54	18.4
Client reporting systems	3.17	67	22.9	3.68	56	19.1
SafeSeaNet	3.02	46	15.7	4.30	44	15.0
Internal reporting system	2.86	13	4.4	4.23	3	1.0
OT system						
Power management systems (PMS)	2.64	18	6.1	4.52	6	2.0
Electronic Chart Display and Information System (ECDIS)	2.93	3	1.0	4.92	1	0.3
Radar	2.10	3	1.0	4.92	1	0.3
Dynamic Position System (DP-system)	2.67	4	1.4	4.97	4	1.4
Remote access for maintenance	3.51	27	9.2	4.09	31	10.6
Cargo and loading management systems	2.01	27	9.2	4.33	19	6.5

*Participants who chose "I don't know/Don't use this" when assessing cyber risks **Participants who chose "I don't know/Don't use this" when assessing system benefits ***System excluded from the analyses

Table 3 Statistics of variables used in the Wilcoxon signed-rank test

	Information	Min	Max	*N*	SD	Mean
Perceived cyber risk IT systems	Mean values of 5 ordinal variables	1.20	5.00	291	.807	3.44
Perceived cyber risk OT systems	Mean values of 6 ordinal variables	1.00	5.00	290	.955	2.69

Table 4 Results of Wilcoxon signed-rank test comparing perceived cyber risk towards OT and IT systems

N	290
T	3279
A	1334.368
Z	−11.970
p (2-sided)	.000
r ($z/\sqrt{N}$)	−.703

5.3 Reliability and validity of measurements

Summative indexes were created to represent the measured constructs by summing the scores of the measured items within each latent variable. An overview of the variables is shown in Table 5. The measured items within the variables cyber risk perception, perceived benefit, and trust are assumed to be indicators of the underlying latent variables, and these items are expected to be correlated [56]. This is not the case with the items within cyber security training and experience with cyber-attacks, which are considered as formative measurements [57].

Internal consistency is often used as a reliability indicator of measurements expected to correlate [56]. Cronbach's alpha coefficient was utilized to assess the reliability of the applicable variables. The reliability analysis results, presented in Table 5, demonstrate the internal consistency of the variables measuring cyber risk perception, perceived benefit, and trust, which all show acceptable levels with Cronbach's alpha values > 0.7. Further, the validity of the measurement instruments was a key consideration. The questionnaire items were developed based on a review of existing literature on risk perception, benefit, and trust [19, 41, 44, 50, 58], ensuring that the constructs of interest were captured.

5.4 Hierarchical regression analysis

Hierarchical regression analysis was performed to test H2. Two separate analyses were conducted for cyber risk perception towards IT and OT systems. Because of theoretical considerations, the first step in the hierarchy included the independent variables perceived benefit and trust. The variables cyber security training and experiences with cyber-attacks were added in the second step.

The regression models with cyber risk perception towards IT systems as dependent variable are conveyed in Table 6.

Table 5 Statistics of variables used in the regression analysis

	Information	Range	Min	Max	*N*	SD	Mode	α
Perceived cyber risk IT systems**	S.I* with 5 ordinal variables	22	3	25	291	4.43	17	.770
Perceived cyber risk OT systems**	S.I* with 6 ordinal variables	27	3	30	290	5.92	14	.880
Perceived benefit	S.I* with 11 ordinal variables	32	23	55	293	6.03	55	.753
Trust	S.I* with 12 ordinal variables	48	12	60	293	7.82	48	.897
Cyber security training	S.I* with 8 ordinal variables	30	5	35	293	5.91	17	
Experience cyber-attack own vessel	Ordinal variable	4	0	4	293	.904	1	
Experience cyber-attack company	Ordinal variable	4	0	4	293	1.02	1	
Hear about cyber-attack others	Ordinal variable	4	0	4	293	1.09	3	

*Summative Index, **Dependent variable

Table 6 Results of hierarchical regression analysis with Cyber Risk Perception of IT systems as dependent variable

	b	SE *B*	β	*p*	95% CI lower	Upper
Step 1						
Constant	6.800	2.071		.001	2.724	10.875
Perceived Benefit	.233	.043	.305	< .001	.138	.309
Trust	−.041	.033	−.072	.223	−.106	.025
Step 2						
Constant	6.889	2.142		.001	2.673	11.104
Perceived Benefit	.198	.045	.270	< .001	.109	.286
Trust	−.052	.034	−.093	.126	−.120	.015
Cyber security training	.083	.046	.110	.072	−.008	.173
Experience cyber-attacks own vessel	.148	.321	.030	.645	−.484	.781
Experience cyber-attacks own company	−.324	.282	−.075	.251	−.879	.230
Heard about cyber-attacks others	.143	.253	.035	.571	−.355	.641

$R^2 = .085$ with $p < .001$ for Step 1; $\Delta R^2 = .016$ with $p = .296$ for Step 2

Table 7 Results of hierarchical regression analysis with Cyber Risk Perception of OT systems as dependent variable

	b	SE *B*	β	*p*	95% CI lower	Upper
Step 1						
Constant	7.197	2.835		.012	1.616	12.778
Perceived Benefit	.211	.059	.216	< .001	.095	.328
Trust	−.027	.046	−.036	.552	−.117	.063
Step 2						
Constant	7.236	2.841		.011	1.644	12.829
Perceived Benefit	.147	.060	.150	.015	.029	.264
Trust	−.053	.045	−.070	.248	−.142	.037
Cyber security training	.142	.061	.142	.020	.023	.262
Experience cyber-attacks own vessel	.966	.427	.147	.024	.126	1.805
Experience cyber-attacks own company	−1.235	.374	−.215	.001	−1.972	−.499
Heard about cyber-attacks others	.749	.336	.138	.027	.088	1.410

$R^2 = .043$ with $p = .002$ for Step 1; $\Delta R^2 = .074$ with $p < .001$ for Step 2

Table 8 Results of multicollinearity analysis

Variables	Tolerance	VIF
Step 1		
Perceived Benefit	.908	1.101
Trust	.908	1.101
Step 2		
Perceived Benefit	.840	1.190
Trust	.861	1.162
Cyber security training	.848	1.179
Experience cyber-attack own vessel	.737	1.357
Experience cyber-attack own company	.737	1.357
Heard about cyber-attack others	.811	1.233

[a]Dependent variable: Cyber risk perception IT systems

Table 9 Results of multicollinearity analysis

Variables	Tolerance	VIF
Step 1		
Perceived Benefit	.908	1.101
Trust	.908	1.101
Step 2		
Perceived Benefit	.840	1.191
Trust	.861	1.162
Cyber security training	.848	1,179
Experience cyber-attack own vessel	.737	1.357
Experience cyber-attack own company	.737	1.357
Heard about cyber-attack others	.810	1.234

[a]Dependent variable: Cyber risk perception OT systems

Perceived benefit significantly related to cyber risk perception of IT systems in both models ($\beta_1 = 0.233, p < 0.001$; $\beta_2 = 0.198$, $p < 0.001$). *Trust*, *cyber security training*, and the three *experience with cyber-attacks* variables were not significant in both steps ($p > 0.05$). Step 1 accounted for 8.5% of the variance ($R^2 = 0.085$). The change in R^2 was not significant in step 2 ($R^2 = 0.101$; $\Delta R^2 = 0.016$, $p = 0.296$), and there was a decrease in the F value ($F_1 = 13.380$; $F_2 = 5.299$), indicating that the addition of the variables in Step 2 led to a decrease in model fit. The F-test is a component of analysis of variance (ANOVA) and is utilized to determine the significance of the overall model [53].

The regression models with the dependent variable of cyber risk perception towards OT systems is presented in Table 7. *Perceived benefit* significantly related to the dependent variable in both steps ($\beta_1 = 0.211$, $p < 0.001$; $\beta_2 = 0.147$, $p = 0.015$), and *trust* was not significant in neither of the models ($p > 0.05$). *Cyber security training* ($\beta = 0.142$, $p = 0.020$), *experience with cyber-attacks towards own vessel* ($\beta = 0.966$, $p = 0.024$) and *company* ($\beta = -1.235$, $p = 0.001$), and *heard about cyber-attacks towards others* ($\beta = 0.749$, p = 0.027) significantly predicted cyber risk perception towards OT systems. The first step accounted for 4.3% of the variance ($R^2 = 0.043$), and the change in R^2 was significant and accounted for 11.8% of the variance in the second step ($R^2 = 0.118$; $\Delta R^2 = 0.074$, $p < 0.001$). Even so, there was a slight decrease in the F value ($F_1 = 6.486$; $F_2 = 6.292$), indicating that the model fit did not improve.

5.5 Multicollinearity

Multicollinearity arises when independent variables have high correlation between themselves, leading to a lack of ability to predict the values of dependent variables [53]. To assess the presence of multicollinearity, both variance inflation factor (VIF) and correlation analysis were conducted. The results, as shown in Table 8 and 9, indicate that all variables have VIF values below three, suggesting low levels of multicollinearity. Moreover, the tolerance levels are above 0.2, indicating that a substantial proportion of variance in each variable is not shared with other predictors. However, the correlation analysis reveals significant correlations between multiple variables (Table 10 and 11). Most correlations are moderate (between 0.2 and 0.4) or weak (> 0.2), except for the correlation between experience with cyber-attacks towards own vessel and company, which demonstrates a correlation coefficient of 0.462 and 0.461. Although the presence of this medium–high correlation is not very surprising and suggests the potential for multicollinearity, the overall VIF values and tolerance levels indicate that the multicollinearity issue in the model might be within acceptable limits. Even so, this could introduce challenges in the regression analysis by reducing the statistical significance of experience with cyber-attacks towards own vessel and company, since they might explain overlapping portions of variance in the dependent variables [56].

6 Summary of results

The statistical analyses gave the following results:

- The result from the Wilcoxon signed-rank test supports H1 and shows that deck officers perceive significantly lower cyber risks towards operational technology than informational technology.
- The results from the hierarchical regression analyses support H2 regarding perceived benefit, cyber security training, and experience with cyber-attacks. Figure 2 visualizes the second step of the regression analyses, showing the difference in significance levels and beta values, suggesting that these independent variables influence deck

Table 10 Correlation analysis with Cyber Risk Perception IT systems as dependent variable

	Cyber risk perception IT	Perceived benefit	Trust	Cyber security training	Experience cyber-attack own vessel	Experience cyber-attack own company	Heard about cyber-attack others
Cyber Risk Perception IT	1.000						
Perceived Benefit	.283**	1.000					
Trust	.020	.303**	1.000				
Cyber security training	.172*	.285**	.206**	1.000			
Experience cyber-attack own vessel	.032	.040	.032	.156*	1.000		
Experience cyber-attack own company	−.039	−.050	−.125*	.125*	.462**	1.000	
Heard about cyber-attack others	.091	.140*	−.050	.234**	.331**	.306**	1.000

*$p < 0.05$; **$p < 0.01$

officers' cyber risk perception differently with respect to IT and OT systems.

- The results from the regression analyses do not support H2 regarding trust. Figure 2 shows that trust was not a significant predictor of deck officers' cyber risk perception in either of the regression models.
- Perceived benefit of systems was positively significant for predicting cyber risk perception towards both IT and OT systems, with quite similar beta values. However, this independent variable explains more of the variance in perception of cyber risks towards IT systems than OT systems.
- The amount of cyber security training positively predicts deck officers' perception of cyber risks towards OT systems but was not a significant predictor towards IT systems.
- Previous experience with cyber-attacks towards own vessel and company were significantly related to cyber risk perception of OT systems but not of IT systems. Figure 2 shows that deck officers with experience of cyber-attacks towards own vessel have an increase in their cyber risk perception, and a decrease in their cyber risk perception if they have experience with cyber-attacks towards own company.
- If deck officers have heard about other vessels or companies being victims of cyber-attacks, it positively predicts their cyber risk perception of OT systems.

7 Discussion

The aim of this research is to study deck officers' cyber risk perception. The goals were to measure if (1) deck officers perceive lower cyber risks towards OT systems than IT systems and investigate if (2) there is a difference in how perceived benefit, trust, cyber security training, and experience with cyber-attacks predict their perception of cyber risks towards IT and OT systems. In this section, the results are reviewed in relation to these goals. Additionally, implications of the work are discussed, recommendations are made, future research areas identified, and limitations considered.

7.1 Level of cyber risk perception towards IT and OT systems

Historically, operational technology on vessels have been isolated from the internet and shielded from cyber threats. This air gap is not the case anymore, and over the past years there has been an extensive increase in cyber-attack vectors and cyber risks towards all maritime systems [3]. Even so, the Wilcoxon signed-rank test result in Table 4 show that deck officers perceive significantly lower cyber risks towards OT systems than IT systems. This discrepancy in level of cyber risk perception might be explained by the systems nature and primary functions since administrative systems are more

Table 11 Correlation analysis with Cyber Risk Perception OT systems as dependent variable

	Cyber risk perception OT	Perceived benefit	Trust	Cyber security training	Experience cyber-attack own vessel	Experience cyber-attack own company	Heard about cyber-attack others
Cyber Risk Perception OT	1.000						
Perceived Benefit	.205**	1.000					
Trust	.029	.303**	1.000				
Cyber security training	.199**	.285**	.205**	1.000			
Experience cyber-attack own vessel	.120*	.040	.033	.157*	1.000		
Experience cyber-attack own company	−.085	−.050	−.125*	.126*	.461**	1.000	
Heard about cyber-attack others	.179**	.140*	−.051	.234**	.332**	.307**	1.000

*p < 0.05; **p < 0.01

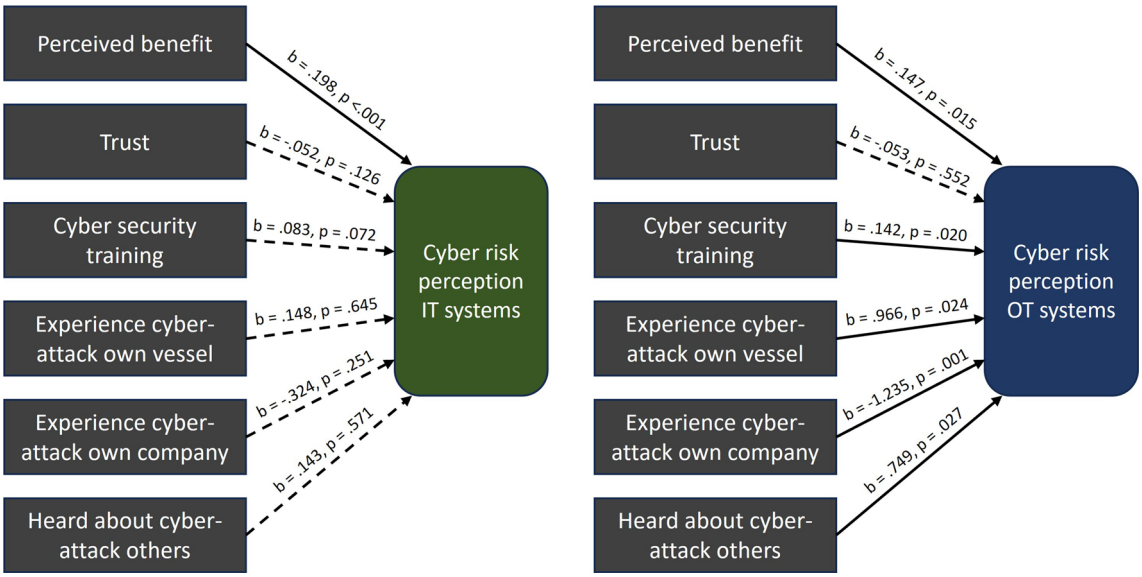

Fig. 2 Results of the causal relationship between the independent variables and cyber risk perception in the second step of the hierarchical regression analyses. Dotted line indicates no significant relationship. Beta value and significance level are given for each independent variable

associated with cyber-attacks and security needs than operational systems [26]. Moreover, there is no obligation of reporting maritime cyber-attacks to the authorities, and the fear of reputation loss might deter the shipping companies from reporting cyber incidents [5]. Therefore, if deck officers only rely on the available examples of previous cyber-attacks to inform their risk perceptions, it might lead to an underestimation of cyber risks towards their operational technology [50].

Another aspect concerns how the officers assessed cyber risks when answering the questionnaire. If potential consequences of cyber-attacks towards their vessels operational technology seems somewhat abstract, they might think of probability more than fatal consequences when assessing the level of cyber risk towards OT systems [17]. Media coverage of cyber-attacks with fatal consequences for maritime companies are mostly related to attacks on IT-infrastructure [7]. This could be substantiated with findings indicating that

vessels are not perceived as attractive targets for cyber criminals, and that the onboard crew feels in control of their operational technology [19]. Nevertheless, the significant differences in cyber risk perception levels towards IT and OT systems demonstrate the importance of investigating what factors influence these perceptions.

7.2 Factors influencing cyber risk perception

Previous research has explored the predictive power of factors for perceived risk in cyber security. However, it has not been investigated in a maritime context before [8, 11]. It is essential to gain insight into specific contexts where people use technology, as factors explaining perception of risk varies from population to population and from profession to profession [35]. The results of the two regression models in this study show a difference in predictive power and significance of independent variables. This substantiates the notion that deck officers perceive cyber risks differently towards IT- versus OT systems, and that factors influence these perceptions at varying degrees. Knowledge of this will impact how the maritime industry should develop training programs, policies, risk communication and design technology to improve cyber security behaviour and compliance [18, 59]. The next sub-sections discuss the findings related to perceived benefit, trust, cyber security training and experience and familiarity with cyber-attacks.

7.2.1 Perceived benefit

Both regression models utilized in the analyses demonstrated that perceived benefit significantly enhances deck officers cyber risk perception. Interestingly, this result contrasts with prior research, which often finds an inverse relationship between perceived cyber risk and benefit [15, 40]. When examining the benefit scores presented in Table 2, it is evident that deck officers perceive high levels of benefit for all systems. Moreover, Table 5 show that the mode for perceived benefit across all systems is the maximum value of 55. These observations indicate that perceived benefit towards IT and OT systems are generally high and might be assessed differently in comparison to alternative contexts and other forms of information technology. A possible explanation for this could stem from the operational and demanding working environment aboard vessels [60]. Deck officers rely extensively on both IT and OT systems to perform their work duties in a safe and efficient manner, leaving them with no viable substitutes for these systems [33]. This might coincide with the notion that, when perceived benefit is high enough, users are more inclined to accept a certain level of associated risk [31, 38].

Preceding studies have asked participants to evaluate the specific risks or benefits of activities associated with the technologies in question [15, 33, 61]. It is plausible that the deck officers would assess cyber risks or benefits of specific tasks, such as navigation with radar or communication by email, in a different manner compared to assessing the overall system cyber risks or benefits of radar and email. Nevertheless, it is important to note that the findings indicate a generally high level of perceived system benefits, and that this perception might, to some extent, contribute to an elevation in deck officers' cyber risk perception. By considering this in cyber risk communication and cyber security training programs, it could provide a more balanced perspective of both system benefits, potential risks, and system vulnerabilities. Consequently, this could facilitate more informed decision-making regarding cyber risk management and strengthened incident response [4, 59].

7.2.2 Trust

Trust did not emerge as a significant predictor of cyber risk perception towards either IT- or OT systems. In assessing trust towards various stakeholders (comprising the crew, company management, IT-department, suppliers, government, and IMO) working with securing these systems, the concepts of social trust and confidence were used. Social trust is related to shared intentions and values, and the results may imply that deck officers perceive a lack of alignment in intentions and values between themselves and the stakeholders concerning cyber security matters [35, 58]. Alternatively, it could suggest that the stakeholders are a highly diverse group, making it challenging to identify a collective set of shared values between them.

Confidence, on the other hand, hinges on past experiences over time and the perceived knowledge of stakeholders about the technologies in question [62]. If deck officers have limited cyber security related interactions with the stakeholders, the officers may not have sufficient information or experiences for the development of confidence-based judgements. Overall, the participants might lack substantial positive or negative experience with stakeholders' management of cyber risks towards the onboard systems. This potential absence of experiences to anchor their value and confidence judgements might contribute to the lack of statistically significance of trust.

Furthermore, the divergence between the results observed in this quantitative study and the implications drawn from the previous qualitative study, which underscored the significance of trust in others for cyber defence [19], can be attributed to the complex nature of trust mechanisms. Consequently, trust within maritime cyber security could be evaluated differently regarding value perspectives and importance attributed to stakeholders' knowledge [35, 63]. The results are also influenced by how social trust and confidence were operationalized in the questionnaire. It is possible that the questions did not fully capture the nuances of how deck

officers perceive trust in this context, or that trust has an indirect impact on cyber risk perceptions. Future research should explore these trust dynamics and possible correlations comprehensively. Furthermore, it may be worthwhile to investigate the relevance of trust dimensions within security research as well, such as self-efficacy and control, technical trust, and the potential impact of limited personal interaction [64].

7.2.3 Cyber security training

The results show that the amount of cyber security training deck officers receive, positively predicts their cyber risk perception towards OT systems but has no significant impact on their perception of cyber risks towards IT systems. Since knowledge-building within maritime cyber security can be seen as novel, the main part of this training has been theoretical and focusing on IT-security [19, 26]. However, maritime personnel depend on operational training and drills to ensure effective crisis management aboard vessels [13]. Since operational technology can be deemed more critical to vessels' operations, increased training related to securing this technology may enhance the deck officers' awareness of OT systems vulnerabilities. Together with a focus on good security behaviours and positive stimuli, this training might lead to more compliant security behaviour, reducing the gap between perceived importance of cyber security and actual cyber-practices [24, 65].

Furthermore, the effectiveness of security methods depends on individuals implementing and using them [61], which in turn makes it important how deck officers comprehend the information given to them about potential cyber risks and threats [65]. Previous research show that people tend to react to the effects of cyber-attacks and not the attack itself [18]. Maybe training programmes targeting OT systems are more likely to give deck officers tools to comprehend potential consequences of cyber incidents and handle cyber risks more efficiently, which in turn enhances their cyber risk perception. These findings imply the necessity for an evaluation of the content and effectiveness of current cyber security training programs, as well as highlighting the need for tailored training approaches focusing on operational aspects of vessels' cyber security. Consequently, these results open for further exploration of the relationship between cyber risk perception, training, and the specific characteristics of IT and OT systems in the maritime domain.

7.2.4 Experience and familiarity with cyber-attacks

The results regarding deck officers' previous experience and familiarity with cyber-attacks provide insights into how personal experiences and external information might shape their cyber risk perception. Again, the results were significant for predicting cyber risk perception towards OT systems but not for IT systems, which further underpins the difference in factors influencing perception of cyber risks towards information and operational technologies.

The observed increase in cyber risk perception towards OT systems among deck officers who have experienced a cyber-attack towards their own vessel, coincides with previous studies finding that personal experience heightens risk perceptions [17, 66]. This increase might be attributed to the availability heuristic, since people tend to perceive risks as high if they find it easy to recall the occurrence of associated events [32, 48, 50]. Conversely, the significant decrease in cyber risk perception among those with experience of cyber-attacks towards their shipping company, could reflect a belief in organisational learning and the company's ability to handle another attack [26].

Furthermore, the positive correlation between familiarity of cyber-attacks towards other vessels or shipping companies and cyber risk perception of OT systems show the influence of external information and mass media [48, 49]. This indicates that deck officers' cyber risk perception is not only influenced by their own experiences, but also by cyber incidents within the maritime industry known through storytelling or media. Even so, the official number of cyber-attacks towards OT systems are much lower than towards IT systems [7], making it important to establish reporting systems for maritime cyber incidents and develop effective awareness campaigns and risk communication tools [67]. More statistical data on maritime cyber incidents would further inform deck officers cyber risk perceptions and support decision making related to cyber risk management [5].

7.3 Implications and practical recommendations

Implications drawn from this empirical study pave the way for strategic recommendations to bridge the gap between theory and practice within maritime cyber security. The findings demonstrate the importance of considering the particularities within maritime cyber risk perception and the essential role of the factors influencing these perceptions. Table 12 summarizes the implications as practical recommendations that can empower operational decision makers to enhance their cyber risk management efforts forward.

7.4 Limitations

This study has some methodological limitations which must be considered. Since the participants in the sample is working within the offshore segment, it might not be possible to generalize the findings to the broader population of deck officers within the maritime industry. Offshore vessels are technically advanced, using a more diverse range of both IT

Table 12 Practical recommendations

Acknowledge the difference between IT and OT systems	The nature of information and operational technology is different, and this influence cyber risk perceptions. Acknowledgement of this difference can aid the process of implementing and revising cyber risk management strategies
Increased collaboration between maritime stakeholders	Increase stakeholders' communications related to cyber security decisions and actions. Emphasize the need for open dialogues, feedback sharing and joint efforts to address cyber risks within the maritime value chain
Specific risk communication tools for IT and OT systems	Develop specific risk communication tools for IT and OT systems with strategies that provide relevant and timely information about cyber incidents. Give transparent and contextually rich information about incidents involving vessels, shipping companies and other maritime companies. Focus on rewarding compliance and good security behaviour
Tailored cyber security training programmes with operational focus	Revise current cyber security training programmes to ensure a focus on operational training and OT systems. Consider the importance of continuous training and learning approaches to strengthen management strategies and cyber incident responses
Cyber incident reporting system	Work to establish structured incident reporting mechanisms to capture cyber incidents, impacts and lessons learned. More comprehensive data of industry-wide incident trends will support more efficient and accurate decision-support tools for cyber risk assessments
Substantiated and holistic cyber security policies	Create holistic policies to substantiate these cyber security recommendations. Highlight the importance of policymaking for enhanced decision making and cyber risk management

and OT systems than for example tankers, dry bulk vessels or ferries [52].

The current study has a cross-sectional design, so it only captures a snapshot of participants' perceptions and experiences at a specific point in time. Longitudinal research may better test and assess the stability of cyber risk perceptions over time [53]. Furthermore, when using questionnaires there is the potential for self-reporting bias. This means participants might provide responses they believe to be socially correct or that align with their roles, possibly resulting in the self-reporting measures not fully capturing the participants' actual perceptions or experiences [56]. Other potential biases in this study could be related to the questionnaire wording or how the constructs were measured and operationalized. Future studies should carefully consider how to measure trust, and investigate the causal, and possible confounding, relationship between trust and perceived benefit.

The explanation percentages in both regression models were low, suggesting that other variables might be more important in explaining deck officers cyber risk perception. This could be because people's perception of cyber risks might deviate from their perception of offline risks, e.g., risks related to gene technology and nuclear power. These offline risks can be replaced with other solutions or avoided if preferred, but IT and OT systems are not replaceable and deck officers depend on these technologies to do their job [33]. This distinction between offline and online risks might cause differences in how attitudes and risk responses are developed. Consequently, it is quite plausible that other variables and mechanisms are affecting people's perceptions of risks in cyberspace versus real life.

8 Conclusion

The empirical evidence in this study show that deck officers perceive cyber risks towards information and operational technology differently. Moreover, the varied influence of perceived benefit, trust, cyber security training, and experience with cyber-attacks provide insights into the intricate interplay of variables influencing cyber risk perceptions. The implications of these distinct findings for IT and OT systems calls attention to the necessity of tailored risk communication tools, cyber security training programs, reporting systems, and holistic cyber security policies within the maritime domain. Future research should analyse the long-term effects of such cyber security interventions, as understanding the causes and effects of the recommended security measures will be crucial.

In conclusion, this study marks a significant stride towards comprehending maritime decision-makers' cyber risk perceptions of technological systems used in highly operational work environments. This previously unexplored perceptive provides an understanding of that human cognition not only distinguishes cyber risks between different contexts but also among different system categories. The hope is that insights provided from this study stimulate further investigations into the complex relationship between human behaviour and maritime technologies within the realm of cyberspace. Capturing a wider understanding of these dynamics will aid in the ongoing efforts to maintain vessel security and safety in this new cyber threat landscape.

Author contributions All authors contributed to the study conception and design. Data collection and analysis were performed by M.H.S. The draft of the manuscript was written by M.H.S and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital). This study was funded by the Grant from the Research Based Innovation Centre "SFI Marine Operation in Virtual Environment (SFI-MOVE)" by the Norwegian Research Council under Project 237929.

Data availability The datasets generated and analysed during the current study are not publicly available due to individual privacy concerns but are available from the corresponding author on reasonable request.

Declarations

Competing interests The authors declare no competing interests.

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

Appendix

Questionnaire with wording, sequence of questions and options:

Variables	Information and question wording	Scaled items	Options/Scales with values in dataset
Age			19–29
			30–39
			40–49
			50–59
			60–69
Gender			Male
			Female
			Other/ Do not want to say
Rank	What is your current rank?		Captain
			Chief mate
			Second mate
			Free text reply
Sailing years	How many years of sailing experience do you have?		
Education	What education do you have?		Vocational school
			Bachelor's degree
			Master's degree

Variables	Information and question wording	Scaled items	Options/Scales with values in dataset
Perceived benefit	As deck officer, you depend on technological systems in your everyday working life. Consider the level of benefit the systems below have for conducting your job On a scale from one to five, where five is very high benefit, how do you assess the benefits of the following systems for your job as a deck officer?	Power management systems (PMS) E-mail Electronic Chart Display and Information System (ECDIS) Radar Passenger servicing and management systems Remote access for maintenance Dynamic Position System (DP-system) Client reporting systems Remote access for monitoring SafeSeaNet Cargo and loading management systems Internal reporting system	1. Very low benefit 2 3 4 5. Very high benefit 0. Don't know/Don't use this
Experience with cyber-attacks	How many times have you experienced a cyber-attack towards any of the vessels you have worked on? How many times have you experienced a cyber-attack towards shipping companies you have worked for? How many times have you heard about other shipping companies or vessels being victim of a cyber-attack?		1. Never 2. One time 3. A few times (about 2–5) 4. Many times (6 + times) 0. I don't know
Cyber security training	How often have you conducted the following cyber security training?	Computer based training (E.g., Seagull CBT) External course Internal course Security drills Tabletops Phishing campaigns on email Awareness campaigns on email Another form for cyber security training	1. Never 2. Once 3. Yearly 4. Twice a year 5. Monthly 0. I don't know

Variables	Information and question wording	Scaled items	Options/Scales with values in dataset
Perceived cyber risk	Cyber risks are caused by threats like malicious software or hackers. These threats exploit cyberspace and may cause cyber incidents towards the systems on board your vessel On a scale from one to five, where five is very high risk, how do you assess the cyber risks towards the following systems?	Power management systems (PMS) E-mail Electronic Chart Display and Information System (ECDIS) Radar Passenger servicing and management systems Remote access for maintenance Dynamic Position System (DP-system) Client reporting systems Remote access for monitoring SafeSeaNet Cargo and loading management systems Internal reporting system	1. Very low cyber risk 2 3 4 5. Very high cyber risk 0. Don't know/Don't use this
Confidence	Consider your level of trust in the institution or persons competence to perform the cyber security related tasks they are responsible for What is your level of trust in the following institutions or persons ability to contribute to the securing of the onboard systems against cyber risks?	Your crew Management in your shipping company IT-department in your shipping company Suppliers of onboard systems Government IMO (International Maritime Organization)	1. No trust at all 2 3 4 5. Very high trust
Social trust	Consider your level of trust in that the institutions or persons don't want to harm you, but are acting in your best interest when performing the cybersecurity tasks they are responsible for What is your level of trust in the following institutions or persons that they are acting in your best interest when it comes to securing the onboard systems against cyber risks?	Your crew Management in your shipping company IT-department in your shipping company Suppliers of onboard systems Government IMO (International Maritime Organization)	1. No trust at all 2 3 4 5. Very high trust

References

1. NORMACyber: NORMA Cyber Annual Threat Assessment 2023 (2023). Available from: https://www.normacyber.no/news/48o1qpgi66klzqspdg7jg3kwta3172.
2. Tam K, Jones K.: Situational awareness: Examining factors that affect cyber-risks in the maritime sector (2019). Available from: https://pearl.plymouth.ac.uk/handle/10026.1/14948
3. DNV: Maritime Cyber Priority 2023 (2023). Available from: https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html
4. Kuhn, K., Bicakci, S., Shaikh, S.A.: COVID-19 digitization in maritime: understanding cyber risks. WMU J. Marit. Aff. **20**(2), 193–214 (2021). https://doi.org/10.1007/s13437-021-00235-1
5. Schinas O, Metzger D.: Cyber-seaworthiness: A critical review of the literature. Marine Policy. 151105592 (2023). https://doi.org/10.1016/j.marpol.2023.105592
6. Ben Farah, M.A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., et al.: Cyber security in the maritime industry: a systematic survey of recent advances and future trends. Information **13**(1), 22 (2022). https://doi.org/10.3390/info13010022
7. Meland PH, Bernsmed K, Wille E, Rødseth ØJ, Nesheim DA.: A retrospective analysis of maritime cyber security incidents. 519–30 (2021). https://doi.org/10.12716/1001.15.03.04
8. Bolbot V, Kulkarni K, Brunou P, Banda OV, Musharraf M.: Developments and research directions in maritime cybersecurity: a systematic literature review and bibliometric analysis. Int. J. Critical Infrastruct. Protection. 39100571 (2022). https://doi.org/10.1016/j.ijcip.2022.100571
9. Kessler GC, Shepard SD.: Maritime Cybersecurity—A Guide for Leaders and Managers. Second Edition edn. Great Britain: Amazon (2022)
10. Erstad E, Ostnes R, Lund MS.: An Operational Approach to Maritime Cyber Resilience. TransNav Int. J. Marine Navigation Safety Sea Transp, pp. 1527–34 (2021). https://doi.org/10.12716/1001.15.01.01
11. Larsen MH, Lund MS.: Cyber risk perception in the maritime domain: a systematic literature review. IEEE Access. 9144895–905 (2021). https://doi.org/10.1109/ACCESS.2021.3122433
12. Erstad E, Lund MS, Ostnes R.: Navigating through cyber threats, a maritime navigator's experience. Appl. Human Factors Ergon. Int. (AHFE International), pp. 5384–91 (2022). https://doi.org/10.54941/ahfe1002205
13. Erstad, E., Hopcraft, R., Vineetha Harish, A., Tam, K.: A human-centred design approach for the development and conducting of maritime cyber resilience training. WMU J. Marit. Aff. **22**(2), 241–266 (2023). https://doi.org/10.1007/s13437-023-00304-7
14. Spencer, T.: Risk perception. Nova Science Publisher, Hauppauge (2016)
15. Van Schaik P, Renaud K, Wilson C, Jansen J, Onibokun J.: Risk as affect: The affect heuristic in cybersecurity. Comput. Security., p. 90101651 (2020). https://doi.org/10.1016/j.cose.2019.101651
16. Sjöberg L, Moen B-E, Rundmo T.: Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research. Rotunde publikasjoner Rotunde, pp. 8455–8476 (2004).
17. Van Schaik P, Jeske D, Onibokun J, Coventry L, Jansen J, Kusev P.: Risk perceptions of cyber-security and precautionary behaviour. Comput. Human Behav., pp. 75547–75559. (2017). https://doi.org/10.1016/j.chb.2017.05.038
18. Bada M, Nurse JR.: The social and psychological impact of cyber-attacks. Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press, pp. 73–92 (2020). https://doi.org/10.1016/B978-0-12-816203-3.00004-6
19. Larsen MH, Lund MS, Bjørneseth FB.: A model of factors influencing deck officers' cyber risk perception in offshore operations. Maritime Transp. Res., p. 3100065 (2022). https://doi.org/10.1016/j.martra.2022.100065
20. Haugli-Sandvik M, Pareliussen B, Bjørneseth FB.: Kommunikasjon og distribuert situasjonsbevissthet i maritime fjernoperasjoner. Nyskaping: Fjordantologien 2023. Universitetsforlaget, pp. 269–85 (2023). https://doi.org/10.18261/9788215069371-23-15
21. Refsdal A, Solhaug B, Stølen K.: Cyber-risk management. Springer. 9–47 (2015). https://doi.org/10.1007/978-3-319-23570-7_5
22. Von Solms R, Van Niekerk J.: From information security to cyber security. Comput. Security, pp. 3897–102 (2013). https://doi.org/10.1016/j.cose.2013.04.004
23. Lee AR, Wogan HP., Editors: All at sea: The modern seascape of cybersecurity threats of the maritime industry. OCEANS 2018 MTS/IEEE Charleston (2018). IEEE.
24. Knight V, Sadok M., Editors: Is cyber-security the new lifeboat? An exploration of the employee's perspective of cyber-security within the cruise ship industry. In: 7th International Workshop on Socio-Technical Perspective in IS Development (2021). CEUR Workshop Proceedings
25. Potamos G, Theodoulou S, Stavrou E, Stavrou S., (eds): Building Maritime Cybersecurity Capacity Against Ransomware Attacks. Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media. Cyber Science 2022; 20–21 June. Wales (2023). Springer
26. Chubb N, Finn P, Ng D.: The Great Disconnect (2022). Available from: https://safety4sea.com/wp-content/uploads/2022/03/Thetius-hfw-cyberowl-Great-disconnect-cyber-risk-management-2022_03.pdf
27. Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., Michaloliakos, M.: Cybersecurity challenges in the maritime sector. Network **2**(1), 123–138 (2022). https://doi.org/10.3390/network2010009
28. Alcaide JI, Llave RG.: Critical infrastructures cybersecurity and the maritime sector. Transp. Res. Proc., pp. 45547–54 (2020). https://doi.org/10.1016/j.trpro.2020.03.058
29. Slovic, P.: Perception of risk: Reflections on the psychometric paradigm. Praeger, Theories of Risk. New York (1990)
30. Kahneman D, Slovic SP, Slovic P, Tversky A.: Judgment under uncertainty: Heuristics and biases. Cambridge university press (1982)
31. Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., Combs, B.: How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. Policy. Sci. **9**(2), 127–152 (1978). https://doi.org/10.1007/BF00143739
32. Siegrist, M., Árvai, J.: Risk perception: Reflections on 40 years of research. Risk Anal. **40**(S1), 2191–2206 (2020). https://doi.org/10.1111/risa.13599
33. Sjöberg, L., Fromm, J.: Information technology risks as seen by the public. Risk Anal. **21**(3), 427–442 (2001). https://doi.org/10.1111/0272-4332.213123
34. Siegrist, M., Keller, C., Kiers, H.A.: A new look at the psychometric paradigm of perception of hazards. Risk Anal. Int. J. **25**(1), 211–222 (2005). https://doi.org/10.1111/j.0272-4332.2005.00580.x
35. Siegrist, M.: Trust and risk perception: A critical review of the literature. Risk Anal. **41**(3), 480–490 (2021). https://doi.org/10.1111/risa.13325
36. Slovic, P.: Perception of risk. Science **236**(4799), 280–285 (1987). https://doi.org/10.1126/science.3563507
37. Starr C.: Social benefit versus technological risk. Science. 1232–8 (1969)
38. LeBlanc D, Biddle R., Editors: Risk perception of internet-related activities. In: 2012 Tenth Annual International Conference on Privacy, Security and Trust (2012). IEEE.

39. Farahmand, F., Spafford, E.H.: Understanding insiders: An analysis of risk-taking behavior. Inf. Syst. Front. **15**(1), 5–15 (2013). https://doi.org/10.1007/s10796-010-9265-x
40. Frewer, L.J., Howard, C., Shepherd, R.: Understanding public attitudes to technology. J. Risk Res. **1**(3), 221–235 (1998). https://doi.org/10.1080/136698798377141
41. Siegrist, M., Cvetkovich, G., Roth, C.: Salient value similarity, social trust, and risk/benefit perception. Risk Anal. **20**(3), 353–362 (2000). https://doi.org/10.1111/0272-4332.203034
42. Rousseau, D.M., Sitkin, S.B., Burt, R.S., Camerer, C.: Not so different after all: a cross-discipline view of trust. Acad. Manag. Rev. **23**(3), 393–404 (1998). https://doi.org/10.5465/amr.1998.926617
43. Earle, T.C., Siegrist, M.: On the relation between trust and fairness in environmental risk management. Risk Anal. Int. J. **28**(5), 1395–1414 (2008). https://doi.org/10.1111/j.1539-6924.2008.01091.x
44. Van Kleef, E., Fischer, A.R., Khan, M., Frewer, L.J.: Risk and benefit perceptions of mobile phone and base station technology in Bangladesh. Risk Anal. Int. J. **30**(6), 1002–1015 (2010). https://doi.org/10.1111/j.1539-6924.2010.01386.x
45. Siegrist, M., Earle, T.C., Gutscher, H.: Test of a trust and confidence model in the applied context of electromagnetic field (EMF) risks. Risk Anal. Int. J. **23**(4), 705–716 (2003). https://doi.org/10.1111/1539-6924.00349
46. Visschers, V.H., Siegrist, M.: How a nuclear power plant accident influences acceptance of nuclear power: results of a longitudinal study before and after the Fukushima disaster. Risk Anal. Int. J. **33**(2), 333–347 (2013). https://doi.org/10.1111/j.1539-6924.2012.01861.x
47. Slovic, P.: Perceived risk, trust, and democracy. Risk Anal. **13**(6), 675–682 (1993). https://doi.org/10.1111/j.1539-6924.1993.tb01329.x
48. Kahneman D.: Thinking, fast and slow. Macmillan (2011)
49. Tversky, A., Kahneman, D.: Judgment under uncertainty: heuristics and biases: biases in judgments reveal some heuristics of thinking under uncertainty. Science **185**(4157), 1124–1131 (1974). https://doi.org/10.1126/science.185.4157.1124
50. De Smidt, G., Botzen, W.: Perceptions of corporate cyber risks and insurance decision-making. Geneva Papers Risk Insurance Issues Pract. **43**(2), 239–274 (2018). https://doi.org/10.1057/s41288-018-0082-7
51. Tversky, A., Kahneman, D.: Availability: A heuristic for judging frequency and probability. Cogn. Psychol. **5**(2), 207–232 (1973). https://doi.org/10.1016/0010-0285(73)90033-9
52. Karan C.: What are Offshore Vessels?. Marine Insight (2019). Available from: https://www.marineinsight.com/types-of-ships/what-are-offshore-vessels/. Last accessed: 07.08.23
53. Field, A.: Discovering statistics using IBM SPSS statistics 5ed. Sage Publications Ltd, London (2018)
54. Gulbrandsen A.: Informasjonssikkerhet og risikovurdering for Nettskjema. University of Oslo (2017). Available from: https://www.uio.no/tjenester/it/adm-app/nettskjema/mer-om/informasjonssikkerhet/. Last accessed: 02.08.23
55. IMO: Women in Maritime (2023), Available from: https://www.imo.org/en/ourwork/technicalcooperation/pages/womeninmaritime.aspx. Last accessed: 07.08.23
56. Ringdal K.: Enhet og Mangfold. 4 ed. Bergen: Fagbokforlaget (2018)
57. Diamantopoulos, A., Winklhofer, H.M.: Index construction with formative indicators: an alternative to scale development. J. Mark. Res. **38**(2), 269–277 (2001). https://doi.org/10.1509/jmkr.38.2.269.188
58. Siegrist, M.: The influence of trust and perceptions of risks and benefits on the acceptance of gene technology. Risk Anal. **20**(2), 195–204 (2000). https://doi.org/10.1111/0272-4332.202020
59. Farahmand F, Dark M, Liles S, Sorge B., Editors: Risk perceptions of information security: A measurement study. In: 2009 International Conference on Computational Science and Engineering (2009). IEEE
60. Hystad, S., Nielsen, M., Eid, J.: The impact of sleep quality, fatigue and safety climate on the perceptions of accident risk among seafarers. Eur. Rev. Appl. Psychol. **67**(5), 259–267 (2017). https://doi.org/10.1016/j.erap.2017.08.003
61. Huang D-L, Rau P-LP, Salvendy G.: Perception of information security. Behav. Inf. Technol. **29**(3), 221–32 (2010). https://doi.org/10.1080/01449290701679361
62. Earle TC, Siegrist M, Gutscher H.: Trust, Risk Perception and the TCC Model of Cooperation 1. Trust in cooperative risk management. Routledge, pp. 1–50 (2012)
63. Earle, T.C.: Trust in risk management: a model-based review of empirical research. Risk Anal. Int. J. **30**(4), 541–574 (2010). https://doi.org/10.1111/j.1539-6924.2010.01398.x
64. Flowerday S, Von Solms R., Editors: Trust: An element of information security. In: IFIP International Information Security Conference (2006). Springer
65. He, W., Zhang, Z.: Enterprise cybersecurity training and awareness programs: Recommendations for success. J. Organ. Comput. Electron. Commer. **29**(4), 249–257 (2019). https://doi.org/10.1080/10919392.2019.1611528
66. Kostyuk N, Wayne C.: The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. J. Glob. Security Stud. **6**(2), ogz077 (2021). https://doi.org/10.1093/jogss/ogz077
67. Tsohou A, Karyda M, Kokolakis S.: Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. Comput. Security, pp. 52128–52141 (2015). https://doi.org/10.1016/j.cose.2015.04.006